ISSN: 2661-3719(Print); 2661-3727(Online)

国密算法与国际标准兼容性提升的生物特征数据加密算法研究

郭宇川

荆州学院　湖北省荆州市　434020

摘　要：随着信息安全方面的需求持续提升，生物特征数据已然成为一种极为重要的身份认证方式，在各类安全系统当中得到了广泛运用。本研究精心提出了一种全新的生物特征数据加密算法，采用将国密算法和国际标准加密算法相互结合的模式，进而设计出了一种优化方案，目的在于提高该算法在多平台、多环境之下的互操作性以及数据安全性。经过研究可以发现，通过对加密算法的关键技术加以改进，是能够切实有效地实现国密算法与国际标准算法之间的兼容互通的，从而确保生物特征数据无论是在国内环境还是在国外环境下，都可以实现安全传输以及安全使用。这一项研究不但为我国信息安全技术的自主创新给予了理论层面的有力支持，而且还为生物特征数据的加密传输提供了更为安全并且兼容性更强的有效解决方案，其应用价值以及实践意义都是十分重要的。

关键词：国密算法；生物特征数据加密；加密算法兼容性

引言

生物特征数据于现代安全认证体系里，正占据着越发关键的地位。生物特征数据有着独特性以及高度个性化的特点，正因如此，其在身份认证、访问控制还有支付安全等诸多领域，都获得了极为广泛的应用。伴随信息化进程不断加快的态势，针对生物特征数据的保护需求，也在逐步地提升起来。国密算法作为一种高强度的加密技术，已经成功地在航天数据保护方面得以应用，并且充分显示出它在高敏感性领域所具备的潜力。所以，去探寻那种适用于生物特征数据的加密技术，同时提升国密算法和国际标准之间的兼容性，这已然成为了当前加密技术研究领域的一个重要的方向。

1 国密算法概述与优势

1.1 国密算法的技术特点与应用

国密算法乃是我国自主展开研发工作而形成的加密算法体系，它具备十分独特的技术方面的优势。其最为核心的优势就体现在算法设计环节所呈现出来的安全性以及效率这两个方面。国密算法运用了相较而言更为复杂一些的加密机制，比如说基于椭圆曲线的那种加密方法，它在抵御攻击的表现上是相当出色的，而且在加密以及解密过程当中所涉及到的计算效率方面同样具备优势，能够在切实保证数据安全的基础之上，颇为显著地提升加解密的速度。尤其是处于数据传输以及存储这样的具体场景之中的时候，国密算法可以有效地去减轻因为加密操作而引发的性能方面的负担。

随着信息安全需求的不断提升，国密算法的应用范围将进一步扩大，特别是在国际标准加密算法逐渐趋同的背景下，探索如何提升国密算法的兼容性，已成为技术发展的重要方向。

1.2 国密算法在生物特征数据加密中的应用前景

国密算法应用于生物特征数据加密，前景颇为广阔。当下，生物特征识别技术得到了广泛运用，在此情形下，指纹、面部识别以及虹膜等各类生物特征数据的采集与存储，慢慢变成了信息安全领域中极为重要的组成部分。这些数据自身带有独特性和敏感性的特点，所以要确保它们的安全性，这无疑是加密技术所要应对的重大挑战。国密算法有着高效的加解密性能，同时抗攻击能力也很出色，在对生物特征数据予以保护这件事上，展现出了独有的优势。尤其是在数据存储以及传输的环节当中，国密算法可以有效提升加密处理的速度，如此一来，便能避免传统加密算法因计算负担过重而产生的性能瓶颈问题。

相较于国际标准加密算法而言，国密算法在针对生物特征数据开展加密工作之时，切实提供了颇为可观的安全性保障，而且能够充分确保在契合国内相关规定的情形下，有效满足特定的数据保护方面的各项需求。与此同时，国密算法在与国内网络环境相互适应的进程当中，自身还具备了一定程度的灵活性特质，有能力对不同应用场景之中所产生的定制化加密相关要求予以有力支持。伴随国际标准加密算法

和国密算法两者之间兼容性相关问题逐步得以妥善解决，在未来的发展阶段，国密算法是很有希望能够在全球范围之内被广泛应用于生物特征数据加密这一领域的，进而有力推动我国在信息安全领域当中实现技术层面的自主创新，并促使我国在国际上的影响力获得显著提升。

2 国际标准加密算法概述与兼容性问题

2.1 国际标准加密算法的现状与发展

国际标准加密算法大体涵盖了对称加密算法、非对称加密算法以及哈希算法等不同类型。其中，像 AES（也就是高级加密标准）这样的对称加密算法，在数据传输以及存储保护方面有着颇为广泛的应用。它有着加密速度快的特点，并且对计算资源的需求也不算高，所以在银行、金融以及企业的数据安全领域经常能见到它的身影。而非对称加密算法，比如 RSA 和 ECC（椭圆曲线加密），它们常常会被用在数字签名以及密钥交换等场景当中。这是因为它们能够提供相对更高的安全性，特别是在那种需要进行身份验证的情形下，就好比在电子邮件以及安全通信协议（像 SSL/TLS）当中。至于哈希算法，是以 SHA 系列作为代表的，其主要用途在于进行数据完整性的校验以及数字签名的生成。伴随着云计算、物联网等新兴技术不断发展起来，国际标准加密算法也慢慢地朝着量子抗性算法、基于硬件的加密解决方案以及更为高效的密钥管理系统去转变了。与此同时，国际标准加密算法也一直在持续改进，以此来应对新冒出来的安全威胁。

2.2 生物特征数据加密中的国际标准应用

在生物特征数据加密这块领域当中，国际标准加密算法的应用重点就体现在对数据的机密性、完整性以及不可否认性等诸多方面加以确保上。像指纹、面部识别、虹膜扫描这类生物特征数据，凭借其自身独特的性质以及不可复制的特点，在身份认证以及安全保护方面得到了极为广泛的运用。生物特征数据所具有的敏感性以及不可更改的特性，也使得加密算法必须得能够切实有效地去应对针对其的保护方面的各种需求，从而避免出现数据泄露以及被篡改的情况。诸如 AES、RSA、ECC 还有 SHA 等国际标准加密算法，在这样的一个过程里面可是发挥出了相当关键的作用。

表 1 不同加密算法的应用对比

加密算法	应用领域	优势	挑战
AES	数据传输与存储保护	高速、高效、低资源消耗	在高安全需求环境下的密钥管理问题
RSA	数字签名与密钥交换	高安全性、适用于身份验证	密钥生成与管理的计算负担
ECC	数字签名与加密通信	高效、安全性好	需要更复杂的密钥生成与管理
SHA	数据完整性校验与数字签名生成	确保数据完整性和认证	与其他加密算法结合时的兼容性问题

2.3 国际标准与国密算法的兼容性问题

在生物特征数据加密这块领域当中，国密算法跟国际标准加密算法二者之间的兼容性方面的问题显得格外突出。国密算法，是我国自主去研发出来的一套密码算法体系，具备着高效以及安全的特点，在国家安全、金融等诸多领域都有着广泛的应用情况。但是国密算法和国际标准加密算法在设计思想方面、加密模式方面以及密钥长度等好些个方面其实是存在着一定的差异的，正因如此，这也就使得它在跨境数据进行交换以及国际合作的这些情境当中面临着一定的兼容性方面的障碍情况。例如，国密算法里的对称加密模式（就像 SM4）和国际上常常会用到的 AES 算法是存在差异的，在加密效率以及安全性这两个方面其实是各有各的长处的，但是由于二者的算法标准并不一样，所以就导致它们在同一个系统里面没办法直接去进行互操作。类似的这种问题在非对称加密算法（比如 SM2）和 RSA、ECC 算法的互操作性方面也是会出现的，特别是在数字签名以及密钥交换的这些个过程当中，不同算法的兼容性方面的问题就显得更加突出了。

3 提升国密算法与国际标准兼容性的方案与实现

3.1 兼容性提升的关键技术

在提升国密算法跟国际标准兼容性的进程当中，关键技术的研究以及实现大多聚焦在算法的适配优化、数据格式的标准化还有密钥管理的协同运作上。起初，鉴于国密算法和国际标准之间存在的差异，得在算法层面去做适配方面的工作。经过对国密算法的数学模型和国际标准加密算法展开对比分析之后，能够提出与之对应的优化办法，让其在计算的复杂程度、加密的强度以及兼容性这些方面达成一种平衡状态。而且数据格式的统一也是极为重要的。不同的加密体系

之下，数据的表示形式是存在差别的，这就使得加密之后的数据没办法在不同的系统当中顺利地完成交换和解密操作。所以，制定出统一的加密数据格式标准，以此来确保在不同标准之间数据具备兼容性，这已然成为提高兼容性的一项核心技术了。针对这样的问题，可以通过去设计新的密钥管理协议的方式，来确保国密算法和国际标准加密算法在密钥的生成、分发、存储以及更新等方面都能具备兼容性。凭借着对这些技术路径进行综合性的应用，就能够在保障数据安全的同时，提升国密算法和国际标准之间的兼容性，进而推动二者在实际应用当中实现无缝对接的效果。

3.2 新型加密算法设计与实现

在设计那种把国密算法和国际标准算法相结合的加密算法之际，其核心想法在于要让这两者既能保住各自的长处，又能实现兼容性以及高效性。要达成这样的目标的话，可以依照模块化的设计思路，把算法自身同密钥管理、数据格式等这类技术要素分离开来，如此一来，在不同的加密体系之下，数据便能够顺利地展开交互以及完成解密操作。有一种常见的策略便是采用多层加密的方案，把国密算法当作是处于核心位置的加密算法，而将国际标准算法作为起到辅助作用的加密手段，借此来填补双方存在的不足之处，进而保证在不同系统之间可以安全地交换数据。

下面是一个结合国密算法与国际标准算法的加密方案示例，其中采用了混合加密机制，先使用国密算法对生物特征数据进行初步加密，再使用国际标准算法对密文进行加密，从而增强兼容性和安全性。

加密流程

```
def hybrid_encryption(data, sm2_public_key, aes_key):
    # 先使用 SM2 加密
    sm2_encrypted_data = sm2_encrypt(data, sm2_public_key)
    # 再使用 AES 加密
    encrypted_data = aes_encrypt(sm2_encrypted_data, aes_key)
    return encrypted_data
示例数据与密钥
data = b”Sensitive biometric data”
sm2_public_key = b”SM2PublicKeyHere” # 国密公钥
aes_key = b”16ByteAESKeyHere” # 16 字节 AES 密钥
执行加密
encrypted_data = hybrid_encryption(data, sm2_public_key, aes_key)
print(“Encrypted Data:”, encrypted_data)
```

这种设计通过将两种加密算法结合，充分利用了国密算法在本地数据保护方面的优势以及国际标准算法在跨国数据交换中的广泛适应性。通过这样的方法，可以在保证数据加密强度的同时，确保加密后的数据能够在不同系统之间进行互操作和兼容。此外，针对算法的实现效率，也可以通过优化加密模式和算法参数，进一步提升系统的性能，确保加密过程在实际应用中的高效性和可行性。

参考文献：

[1] 苏玮 , 殷文浩 , 张文茜 , 等 . 基于国密算法的数据安全管理平台功能设计 [J]. 软件 ,2024,45(05):86-88.

[2] 谭光昭 . 基于国密算法的加密机关键技术研究 [D]. 贵州大学 ,2024.

[3] 折如义 , 段红义 , 姜佩贺 . 安全可控背景下若干国密算法的 FPGA 实现及性能优化 [J]. 电脑编程技巧与维护 ,2023,(12):39-41+61.

[4] 王宏芸 . 基于国密算法的 Fabric 匿名背书方法研究 [D]. 西安理工大学 ,2023.

[5] 张玉俊 . 基于国密算法的高性能 IPSec VPN 网关的研究与实现 [D]. 华北电力大学 (北京),2023.